JOURNAL OF NUMBER THEORY 21, 121–127 (1985)

Free Subgroups in the Group of Units of Group Rings II

JAIRO ZACARIAS GONÇALVES

Instituto de Matemática e Estatística, Universidade de São Paulo, Ag. Iguatemi, C. Postal 20570, São Paulo, Brasil

Communicated by H. Zassenhaus

Received July 1, 1983

Let G be a group, R be the ring of integers of a number field K, RG the group ring of G over R and $U(RG)$ its unit group. We present necessary and sufficient conditions for $U(RG)$ not to contain a free subgroup of rank two when G is finite or the extension of a solvable torsion group by a torsion-free nilpotent group.

1. INTRODUCTION

Let Z be the ring of rational integers and G be a finite group. In [4, Theorem 2], Hartley and Pickel proved that only one of the following three alternatives occurs:

(i) G is abelian

(ii) G is a Hamiltonian 2-group, and $U(ZG) = \{\pm g \mid g \in G\}$

(iii) $U(ZG)$ contains a free subgroup of rank two.

The theorem above motivated the study of when it occurs that $U(KG)$ does not contain a free subgroup of rank two, a question answered in [3]. Now, we propose to investigate what happens when we extend the ring of coefficients to the ring of integers of an algebraic number field.

We prove the following results:

THEOREM A. *Let G be a finite group*

(a) *If K is totally real the following conditions are equivalent*:

(i) *$U(RG)$ does not contain a free subgroup of rank two*

(ii) *$U(RG)$ is nilpotent*

(iii) *$U(RG)$ is FC*

0022-314X/85 $3.00

(iv) *$U(RG)$ is solvable*

(v) $T(U(RG)) = \pm G$

(vi) *$T(U(RG))$ is a subgroup of $U(RG)$*

(vii) *G is an abelian or Hamiltonian 2-group.*

(b) *If K is not totally real, then the following conditions are equivalent:*

(i) *$U(RG)$ does not contain a free subgroup of rank two*

(ii) *G is abelian.*

THEOREM B. *Let G be the extension of a solvable torsion group T by a torsion-free nilpotent group G/T. Then $U(RG)$ does not contain a free subgroup of rank two if, and only if, every idempotent of KT is central in KG and either:*

(i) *K is totally real and T is an abelian or a Hamiltonian 2-group or*

(ii) *K is not totally real and T is an abelian group.*

2. PROOF OF THEOREM A, PART (a)

Let K be a totally real algebraic number field, R the integral closure of Z in K, and $\mathbb{H}_R$ the following subring of the ring of real quaternions

$$\mathbb{H}_R = \{x_1 + x_2 i + x_3 j + x_4 k \mid x_1, x_2, x_3, x_4 \in R\}.$$

For $\alpha = x_1 + x_2 i + x_3 j + x_4 k$, we denote $N(\alpha) = \sum_{m=1}^{4} x_m^2$.

First we prove

PROPOSITION 2.1. *The set of torsion units of $\mathbb{H}_R$ is*

$$T(U(\mathbb{H}_R)) = \{\pm 1, \pm i, \pm j, \pm k\} = K_8.$$

Proof. Let $\alpha = x_1 + x_2 i + x_3 j + x_4 k \in T(U(\mathbb{H}_R))$ be such that $\alpha^n = 1$. Since $N(\alpha)^n = 1$, we conclude that $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1$. We claim that this equation has only trivial solutions.

In fact, let us suppose that x_1 is different from 0 and ± 1. Then some conjugate of x_1 by a Q-monomorphism σ of K has absolute value which is bigger than 1. Therefore $1 = \sigma(x_1)^2 + \sigma(x_2)^2 + \sigma(x_3)^2 + \sigma(x_4)^2 = |(\sigma(x_1)|^2 + |\sigma(x_2)|^2 + |\sigma(x_3)|^2 + |\sigma(x_4)|^2 \geqslant |\sigma(x_1)|^2 > 1$, a contradiction.

LEMMA 2.2. $U(\mathbb{H}_R) = U(R)\, K_8$.

Proof. We will show that the index of $U(R)\, K_8$ in $U(\mathbb{H}_R)$ is equal to one. Let us suppose first that $\sqrt{2} \in R$ and that $[U(\mathbb{H}_R): U(R)K_8] \neq 1$. Then from [8, Theorem 6] and Proposition 2.1 there exists a unit $\xi \in (1+i)K^*$, where $K^* = K - \{0\}$, such that $N(\xi) \notin K^{*2}$. Therefore $\xi = (1+i)\gamma$, $\gamma \in K^*$, and $N(\xi) = 2\gamma^2 = (\sqrt{2}\gamma)^2 \in K^{*2}$, a contradiction.

On the other hand, if $\sqrt{2} \notin R$, we consider the extension $K(\sqrt{2})$ and the integral closure R' of R in $K(\sqrt{2})$. Then, as proved above, we have that $U(\mathbb{H}_{R'}) = U(R')K_8$ and therefore

$$U(\mathbb{H}_R) = U(\mathbb{H}_{R'}) \cap U(\mathbb{H}_R) = U(R')K_8 \cap \mathbb{H}_R = U(R)K_8.$$

Proof of part (a). The equivalence of (iv), (v), (vi), and (vii) was proved in [2, Theorem C], (ii) $\Rightarrow$ (vii), (iii) $\Rightarrow$ (vii), and (i) $\Rightarrow$ (vii) follows by [6, Theorem 1], [7, Theorem VI 5.3] and [4, Theorem 2], respectively.

For the converse, let G be a Hamiltonian 2-group, i.e., $G = E \times K_8$, the direct product of an elementary abelian 2-group E and the quaternion group of order eight. Then we have a monomorphism

$$\Psi\colon R(E \times K_8) \to \bigoplus_{i=1}^{2} \left(\left(\bigoplus_{j=1}^{4} R \right) \oplus \mathbb{H}_R \right)$$

and hence a group monomorphism

$$\begin{aligned} \Psi\colon U(R(E \times K_8)) \to & \prod_{i=1}^{2^{|E|}} \left(\left(\prod_{j=1}^{4} U(R) \right) \times U(\mathbb{H}_R) \right) \\ = & \prod_{i=1}^{2^{|E|}} \left(\left(\prod_{j=1}^{4} U(R) \right) \times U(R)K_8 \right) \end{aligned}$$

by Lemma 2.2. Therefore (vii) $\Rightarrow$ (i), (vii) $\Rightarrow$ (ii), (vii) $\Rightarrow$ (iii).

3. Proof of Theorem A, Part (b)

Let K be a not totally real algebraic number field, R its ring of integers, P the set of finite primes of K, and ∞ the set of infinite primes. Moreover, if $p \in P$, then we denote by K_p the p-adic completion of K and by R_p its ring of integers.

Let $\mathbb{H}$ be the quaternion algebra over K, i.e., $\mathbb{H} = \{x_1 + x_2 i + x_3 j + x_4 k \mid x_1, x_2, x_3, x_4 \in K,\ i^2 = j^2 = -1,\ ij = -ji = k\}$ and Ram $\mathbb{H}$ be the set of primes of K that ramifies in $\mathbb{H}$, i.e., the set of elements of $p \in P \cup \infty$ such that $K_p \otimes_K \mathbb{H}$ is a division ring over K_p.

It is well known that $R = \bigcap_{p \notin \infty} (R_p \cap K)$ and since $\mathbb{H}_R = \{x_1 + x_2 i + x_3 j + x_4 k \mid x_1, x_2, x_3, x_4 \in R\}$ is an R-order of $\mathbb{H}$, we are ready to prove a key fact about $W = \{x \in \mathbb{H}_R \mid N(x) = 1\}$. First we recall

LEMMA 3.1. *Let $GL(2, \mathbb{C})$ be the set of 2×2 matrices over $\mathbb{C}$ whose determinant is different from zero. Then, with the product topology, the set of pairs of matrices that generate free subgroups has nonvoid interior.*

Proof. See [5].

LEMMA 3.2. *The group W contains a free subgroup of rank two.*

Proof. We will consider two cases:

(i) The set of infinite primes of K has at least two elements. For each place $p \in \infty$ let us consider the inclusion $K \hookrightarrow K_p \cong \mathbb{C}$. This induces an embedding $\phi_p: \mathbb{H} \to K_p \otimes_K \mathbb{H} \cong M_2(K_p)$. Now, by restriction to W we have a group monomorphism $\phi: W \to \prod_{p \in \infty, p \notin \operatorname{Ram} \mathbb{H}} SL_2(K_p) \cong \prod_{p \in \infty, p \notin \operatorname{Ram} \mathbb{H}} SL_2(\mathbb{C})$. Now by [9, Theorem IV 1.1(2)] there is a subgroup $G' = \prod_p SL_2(K_p)$ of $G = \prod_{p \in \infty, p \notin \operatorname{Ram} \mathbb{H}} SL_2(K_p)$, $1 \neq G' \neq G$, such that, if π denotes the projection of G over G', in the following commutative diagram

$$\begin{tikzcd} W \arrow[r, "\phi"] \arrow[dr, "\pi \circ \phi"'] & \phi(W) \arrow[r, "\iota"] \arrow[d, "\pi|_{\phi(W)}"] & G \arrow[d, "\pi"] \\ & \pi(\phi(W)) \arrow[r, "\iota"] & G' \end{tikzcd}$$

the map $\pi \circ \phi$ is an isomorphism and $\pi(\phi(W))$ is dense in G'. By Lemma 3.1, $\pi(\phi(W))$ and thus W must contain a pair of matrices which freely generate a free group.

(ii) K is an imaginary quadratic field.

(a) If a is a positive, square free integer, $d > 1$, the Pell–Fermat equation $x^2 - dy^2 = \pm 1$ has a nontrivial solution (a, b), which corresponds to a nontrivial unit of $Z[\sqrt{d}]$. Let $\alpha = a + (b\sqrt{-d})i$ and $\beta = a + (b\sqrt{-d})j$ be elements of $\mathbb{H}_R$. We have that $\alpha, \beta \in U(\mathbb{H}_R)$ and if we argue as in [4, Proposition 1] we deduce that there is an integer n such that α^n and β^n freely generate a free group.

(b) If $K = Q(i)$, then there is an isomorphism $\Psi: \mathbb{H} \to M_2(Q(i))$. Let $\gamma, \delta \in \mathbb{H}$ be such that

$$\Psi(\gamma) = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad \Psi(\delta) = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

Choose an integer $m > 1$ such that $m\gamma, m\delta \in Z[i]$.

Then, if $\alpha = 1 + m\gamma$ and $\beta = 1 + m\delta$, it follows that $\alpha, \beta \in U(\mathbb{H}_R)$,

$$\Psi(\alpha) = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \Psi(\beta) = \begin{bmatrix} 1 & 0 \\ m & 1 \end{bmatrix}.$$

By [1], α and β freely generate a free group.

THEOREM 3.3. *Let G be a noncommutative finite group. Then $U(RG)$ contains a free subgroup of rank two.*

Proof. Suppose this is not so. Then by [3, Theorem 2], G is a Hamiltonian 2-group, i.e., G is the direct product of an elementary abelian 2-group E by the quaternion group K_8, which we write as $K_8 = \langle a, b \mid a^4 = 1, a^2 = b^2, bab^{-1} = a^3 \rangle$. To obtain a contradiction it is enough to show that $U(RK_8)$ contains a free subgroup of rank two.

The function

$$\Psi\colon KK_8 \to K \oplus K \oplus K \oplus K \oplus \mathbb{H}$$
$$\Psi(a) = (1, 1, -1, -1, i)$$
$$\Psi(b) = (1, -1, 1, -1, j)$$

defines an isomorphism of K-algebras. KK_8 has a central primitive idempotent $e = \frac{1}{2}(1 - a^2)$ and the image of $RK_8 e$ by Ψ is $\mathbb{H}_R$. By Lemma 3.2, $U(RK_8 e)$ contains two elements α and β which freely generate a free subgroup. By [4, Lemma 1] there exists a positive integer n such that α^n and β^n belongs to $U(RK_8)\, e$.

Proof of Theorem B. *Necessity.* Since G is solvable, by [7, Theorem VI 4.2] T is an abelian or a Hamiltonian 2-group with every subgroup normal in G.

If K is not totally real, from Theorem A, part (b), it follows that T is abelian. So, it remains to prove that every idempotent of KT is central in KG. We consider two cases:

(i) *K is totally real and T is a Hamiltonian 2-group.* Then argue as in [2, Theorem c]

(ii) *T is abelian.* Suppose not. Then there exist $e = e^2 \in KT$ and $x \in G \backslash T$ which does not centralize e. Since every subgroup of T is normal in G, $A = \langle \operatorname{supp} e \rangle$, the subgroup generated by the support of e, is finite and, without loss of generality, we can assume that $G = \langle x, A \rangle$.

Therefore we have $KA = F_1 \oplus \cdots \oplus F_r$, a direct sum of fields with corresponding primitive orthogonal idempotents $\{e_i\}$. Also, at least one of the e_i's, say e_1, is noncentral. Hence, arguing as in [7, Lemma VI 3.12] there exist an $m>1$ and idempotents $e_2, \ldots, e_m$ such that $e=\sum_{i=1}^{m} e_i$ is a central idempotent of KG, and eKG contains the full matrix ring $M_m(K)$.

Now, let us denote by E_{ij} the $m \times m$ matrix with 1 in its (i, j) entry and zero elsewhere, and let Π: $KG \to eKG$ be the canonical projection. Choose $X_{1m}, X_{m1} \in KG$ such that

$$\Pi(X_{1m}) = E_{1m}, \qquad \Pi(X_{m1}) = E_{m1}.$$

Hence

$$\Pi((1-e_1) X_{m1} e_1) = E_{m1} \qquad \text{and} \qquad \Pi(e_1 X_{1m}(1-e_1)) = E_{1m},$$

since $\Pi(e_1) = E_{11}$.

Choose now an integer $n \geqslant 2$ such that both $\alpha = n(1-e_1) X_{m1} e_1$ and $\beta = n e_1 X_{1m}(1-e_1)$ belong to RG. Then

$$\alpha^2 = \beta^2 = 0,$$

$1+\alpha$ and $1+\beta$ are units of $U(RG)$ and

$$\Pi(1+\alpha) = 1 + nE_{m1}, \qquad \Pi(1+\beta) = 1 + nE_{1m}.$$

As is well known, see [7, Theorem VI 4.2], $\Pi(1+\alpha)$ and $\Pi(1+\beta)$ freely generate a free group, which is a contradiction and proves our claim.

Sufficiency. Imitate the proof of [6, Theorem VI 4.8] to conclude that

$$U(RG) = U(RT) \cdot G,$$

and that $U(RG)$ is solvable.

Acknowledgments

We are indebted to Professor W. Ferrer for a number of useful conversations, and to Professor B. Hartley for pointing out a gap in an earlier version of this paper.

References

1. J. L. Brenner, Quelques groups libres de matrices, *C. R. Acad. Sci. Paris* **241** (1955), 1689–1691.
2. J. Z. Gonçalves, Group rings with solvable unit groups, preprint.
3. J. Z. Gonçalves, Free subgroups of units in group rings, *Canad. Math. Bull.* **27** (1984), 309–312.
4. B. Hartley and P. F. Pickel, Free subgroups in the unit groups of integral group rings, *Canad. J. Math.* **32**, No. 6 (1980), 1342–1352.

5. A. MANDEL AND J. Z. GONÇALVES, Free k-tuples in linear groups, *Bull. Aust. Math. Soc.* **28** (1983), 151–157.
6. C. POLCINO MILIES, Integral group rings with nilpotent unit groups, *Canad. J. Math.* **28** (1976), 954–960.
7. S. K. SEHGAL, "Topics in Group Rings," Dekker, New York, 1978.
8. M. F. VIGNÉRAS, Simplification pour les ordres des corps de quaternions totalement définis, *J. Reine Angew. Math.* **286/287** (1976), 257–277.
9. M. F. VIGNÉRAS, "Arithmétique des algèbres des quaternions," Lecture Notes in Math. Vol. 800, Springer-Verlag, Berlin/Heidelberg/New York, 1980.